REMARKS

This amendment is responsive to the Office Action dated August 21, 2006. In the amendment claims 1-3, 6, 7, 11, 13, 14, 16, 17, 21-25, 28, 29, 33, 35, and 36 have been amended, and claims 1-36 remain pending in the application. Reconsideration of the pending claims in light of these amendments and the following remarks is respectfully requested. Reconsideration and reexamination are respectfully considered.

These amendments add no new matter. The term encryption algorithm is variously used to describe algorithms such as RSA and ECDSA throughout Applicant's specification as filed, and such algorithms are clearly provided as examples of the different algorithms that are executed by the signature modules. For example, these examples are introduced in the Background section of Applicant's specification as filed. (See, e.g., paragraphs 0018-0023 in the published version of the application). These examples are also described in detail in the detailed description, with numerous references to the different encryption algorithms corresponding to different signature modules. (See, e.g., FIG. 21, "RA Management Database" and related description).

Claims 2, 13, 16, 17, 22, 24 and 25 have been rejected under 35 U.S.C. § 112, ¶2, as being indefinite for failing to particularly point out and distinctly claim what Applicant regards as the invention.

Applicant appreciates the Examiner's attention to the claims in this regard. Each of these claims has been amended to remove any perceived ambiguity. Claims 2 and 24 have been amended to clarify that each selected signature module attaches a digital signature to the message data, claims 13, 22 and 35 have been amended to clarify that the signature modules may be configured to execute multiple encryption algorithms, and claims 16 and 17 have been amended to depend from claim 15, which provides antecedent basis for the certificate authority server.

Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims under 35 U.S.C. § 112, ¶2.

Claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 6,035,402 to Vaeth et al. ("Vaeth"). This rejection is traversed.

Independent claim 1 recites: *[a] public key certificate issuing system comprising:*

a certificate authority for issuing a public key certificate used by an entity; and

a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;

wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

These claimed features are neither disclosed nor suggested by Vaeth. Vaeth discloses a "Virtual Certificate Authority" wherein requests for a certificate and verification information are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities. The entity with verification responsibilities is referred to as the registration authority.

First, Applicant submits that Vaeth does not generally describe the sequence of having the registration authority receive a public key certificate issuance request and transmitting the same to the certificate authority. Instead, a requester interfaces with the CA and the RA later participates in the verification process.

However, even assuming that such a feature is presented in Vaeth, there is still no disclosure or suggestion in Vaeth of (1) "*said certificate authority, having a plurality of signature modules each executing a different encryption algorithm*"; (2) selecting "*at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm ...*" as claimed by

Applicant.

In Vaeth, a CA may be configured to provide specialized functions such as for cardholders, merchants, and payment gateways. To do this, the CA may use a variety of crypto cards that respectively "perform the cryptographic aspects of their respective functions, including the generation of the particular type of certificate, which in turn includes the encryption of the digital signature of the "virtual CA" relative to that type of certificate." (Vaeth, at 7:34-47).

These different "respective functions" that may be provided by the crypto cards of Vaeth are apparently directed at the general differences that are required for the different roles. For example, the functions provided by the CA may be different for a cardholder as opposed to a merchant. There is no mention or suggestion of having support for entirely different ***encryption algorithms***, as claimed by Applicant.

Since Vaeth does not disclose different encryption algorithms, it also does not disclose any identification of an assigned encryption algorithm, even generally. Moreover, in no way does Vaeth identify an assigned encryption algorithm with reference to a table that associates the requesting registration authority with an assigned signature algorithm. There is no discussion of any kind in Vaeth regarding a correlation of an encryption algorithm to a given registration authority. The passages relied upon by the Examiner merely indicate that different RAs may access a certificate request and data, that common hardware may support multiple "virtual CA" functions, and that the same RA may act as a different "virtual CA" for different types of certificates. None of these examples offer any suggestion of making a decision as to which encryption algorithm to use by correlating an RA to an encryption algorithm.

Perhaps the Examiner contends that *something* must indicate which CA functionality to apply, and perhaps that is a true statement. However, there are no details as to how this is accommodated, and there is certainly no description of any kind stating or suggesting that the technique claimed by Applicant is used – identifying the encryption algorithm that should be used based upon a table that associates the requesting RA to the encryption algorithm.

Vaeth thus clearly fails to disclose or suggest at least these features of independent claim 1. Independent claims 14, 23, and 36 are also neither disclosed nor suggested by Vaeth for reasons similar to those provided regarding claim 1 above. Furthermore, the rejected dependent claims incorporate the features recited in their respective independent claims, as well as their separately recited, patentably distinct features, and thus are also neither disclosed nor suggested by Vaeth.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 under 35 U.S.C. § 102(b) as being anticipated by Vaeth.

Claims 4, 7, 26 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of U.S. Pat. No. 6,202,157 to Brownlie et al. ("Brownlie"). This rejection is traversed.

Claims 4, 7, 26 and 29 depend either directly or indirectly from the above-described independent claims and thus incorporate the features contained therein. Brownlie discloses a computer network security system, and offers no disclosure or suggestion of having different encryption algorithms, selecting one of the different encryption algorithms, or making such a selection with reference to a table that that associates the registration authority with an assigned signature algorithm, all features that are also absent from Vaeth as described above. Thus, the proposed combination would still fail to yield the features incorporated into these dependent claims, let alone the additional features separately recited therein.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 4, 7, 26 and 29 under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of Brownlie.

Claims 8, 18 and 30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of Boneh et al., "On the Importance of Checking Cryptographic Protocols for Faults" ("Boneh"). This rejection is traversed.

Claims 8, 18 and 30 are also dependent claims that incorporate the features recited in the above-described independent claims. Boneh appears to describe how various authentication protocols can be broken using hardware faults. Clearly, Boneh also offers no disclosure or suggestion of having different encryption algorithms, selecting one of the different encryption algorithms, or making such a selection with reference to a table that that associates the registration authority with an assigned signature algorithm. The proposed combination would still fail to yield the features incorporated into these dependent claims, let alone the additional features separately recited therein.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 8, 18 and 30 under 35 U.S.C. § 103(a) as being unpatentable over Vaeth in view of Boneh.

For the foregoing reasons, reconsideration and allowance of the claims which remain in this application are solicited. If any further issues remain, the Examiner is invited to telephone the undersigned to resolve them.

Dated: November 21, 2006

Respectfully submitted,
By 40,290
Ronald P. Kananen
Registration No.: 24,104
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750
Attorney for Applicant